O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETINING JIZZAX FILIALI

KOMPYUTER ILMLARI VA MUHANDISLIK TEXNOLOGIYALARI

mavzusidagi Xalqaro ilmiy-texnik anjuman materiallari to‘plami

2026-yil 25-26-sentabr

(2-qism)

JIZZAX-2026

Kompyuter ilmlari va muhandislik texnologiyalari. Xalqaro ilmiy-texnik anjuman materiallari to‘plami – Jizzax: O‘zMU Jizzax filiali, 2026-yil 25-26-sentabr. 315-bet.

Xalqaro miqyosidagi ilmiy-texnik anjuman materiallarida zamonaviy kompyuter ilmlari va muhandislik texnologiyalari sohasidagi innovatsion tadqiqotlar aks etgan.

Globallashuv sharoitida davlatimizni yanada barqaror va jadal sur’atlar bilan rivojlantirish bo‘yicha amalga oshirilayotgan islohotlar samarasini yaxshilash sohasidagi ilmiy-tadqiqot ishlariga alohida e’tibor qaratilgan. Zero iqtisodiyotning, ijtimoiy sohalarni qamrab olgan modernizatsiya jarayonlari, hayotning barcha sohalarini liberallashtirishni talab qilmoqda.

Ushbu ilmiy ma’ruza tezislari to‘plamida mamlakatimiz va xorijlik turli yo‘nalishlarda faoliyat olib borayotgan mutaxassislar, olimlar, professor-o‘qituvchilar, ilmiy tadqiqot institutlari va markazlarining ilmiy xodimlari, tadqiqotchilari, magistr va talabalarning ilmiy-tadqiqot ishlari natijalari mujassamlashgan.

Mas’ul muharrirlar: DSc.prof. Turakulov O.X., t.f.n., dots. Baboyev A.M.

Tahrir hay’ati a’zolari: p.f.d.(DSc), prof. Turakulov O.X., t.f.n., dots. Baboyev A.M., t.f.f.d.(PhD), prof. Abduraxmanov R.A., p.f.f.d.(PhD) Eshankulov B.S., p.f.n., dots. Aliqulov S.T., p.f.n., dots. Alimov N.N., p.f.f.d.(PhD), dots. Alibayev S.X., т.f.f.d.(PhD), dots. Abdumalikov A.A, p.f.f.d.(PhD) Hafizov E.A., f.f.f.d.(PhD) dots., Norbekova B.Sh. p.f.f.d.(PhD) dots. Sindorov L.K., t.f.f.d.(PhD), dots. Nasirov B.U., b.f.f.d. (PhD) O‘ralov A.I., p.f.n., dots. Aliqulov S.T., t.f.f.d.(PhD) Kuvandikov J.T., i.f.n., dots. Tsoy M.P., Sharipova S.F., Jo‘rayev M.M.

Mazkur to‘plamga kiritilgan ma’ruza tezislarining mazmuni, undagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligi hamda tanqidiy fikr-mulohazalar, keltirilgan takliflarga mualliflarning o‘zlari mas’uldirlar.

SUN’IY INTELLEKT TIZIMLARIDA AXBOROT XAVFSIZLIGINI TA’MINLASH: MUAMMOLAR, XAVFLAR VA ZAMONAVIY YECHIMLAR

Qudratov Zarif Zohid o‘g‘li 1_sho‘ba
Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universitetining Jizzax filiali
1- bosqich magistranti, Jizzax, O‘zbekiston
E-mail: zarif6460@gmail.com

Annotatsiya: Mazkur maqolada sun’iy intellekt texnologiyalarining jadal rivojlanishi sharoitida axborot xavfsizligini ta’minlash masalalari tahlil qilinadi. Sun’iy intellekt tizimlari katta hajmdagi ma’lumotlarni qayta ishlash, qarorlarni avtomatlashtirish va xizmatlar sifatini oshirish imkonini berayotgan bo‘lsa-da, ular bilan bog‘liq yangi kiberxavflar ham shakllanmoqda. Maqolada ma’lumotlar maxfiyligi, modelga hujumlar, prompt injection, ma’lumotlar zaharlanishi, modelni o‘g‘irlash, sun’iy yaratilgan kontentdan noto‘g‘ri foydalanish hamda inson omili kabi xavflar ko‘rib chiqiladi. Shuningdek, sun’iy intellekt tizimlarida xavfsizlikni loyihalash bosqichidan boshlab joriy etish, kirish huquqlarini boshqarish, ma’lumotlarni minimallashtirish, audit, monitoring va xodimlarning raqamli savodxonligini oshirishga asoslangan yondashuvlar taklif etiladi

Kalit so‘zlar: sun’iy intellekt, axborot xavfsizligi, kiberxavfsizlik, mashinaviy o‘qitish, katta til modellari, ma’lumotlar maxfiyligi, prompt injection, ma’lumotlar zaharlanishi, risklarni boshqarish, kiberhujum.

Kirish

Raqamli transformatsiya jarayonida sun’iy intellekt (SI) texnologiyalari iqtisodiyot, ta’lim, sanoat, tibbiyot, davlat boshqaruvi va xizmat ko‘rsatish kabi ko‘plab sohalarga tez sur’atlarda kirib bormoqda. Sun’iy intellekt asosidagi tizimlar ma’lumotlarni tahlil qilish, tasniflash, prognozlash, matn va tasvir yaratish, texnik jarayonlarni optimallashtirish hamda inson faoliyatini avtomatlashtirishda muhim vositaga aylanmoqda. Shu bilan birga, SI tizimlari oddiy dasturiy ta’minotdan farqli ravishda ma’lumotlar to‘plami, model, algoritm, hisoblash infratuzilmasi va foydalanuvchi o‘zaro aloqasining bir butun majmuasi sifatida faoliyat yuritadi. Mazkur murakkablik xavfsizlikni ta’minlashga yangi talablar qo‘yadi.

Axborot xavfsizligi an’anaviy ravishda maxfiylik, yaxlitlik va mavjudlik tamoyillari bilan ifodalanadi. Shuning uchun SI xavfsizligi faqat antivirus yoki tarmoq himoyasi bilan cheklanmaydi.

Mazkur maqolaning maqsadi sun’iy intellekt tizimlarida uchraydigan asosiy axborot xavfsizligi xatarlarini tizimli ravishda ko‘rib chiqish va ularni kamaytirish bo‘yicha amaliy yondashuvlarni bayon etishdan iborat. Tadqiqot doirasida xavflar texnik, tashkiliy va inson omili nuqtayi nazaridan tahlil qilinadi. Shuningdek, xavfsizlikni boshqarish uchun xalqaro amaliyotda qo‘llaniladigan risklarni boshqarish va kiberxavfsizlik ramkalari bilan uyg‘unlashgan yondashuv taklif etiladi.

1. Sun’iy intellekt va axborot xavfsizligining o‘zaro bog‘liqligi

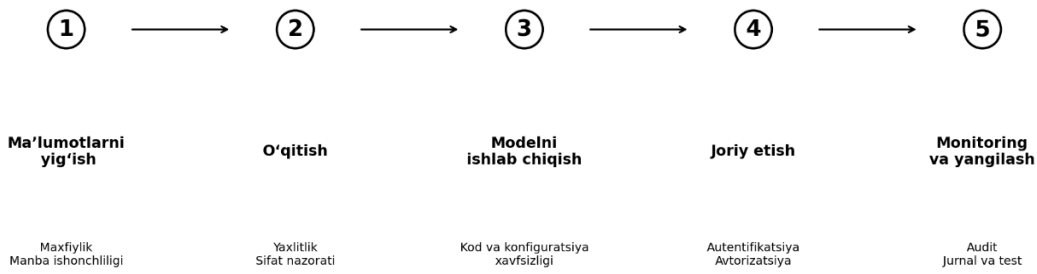
Sun’iy intellekt tizimining xavfsizligi uning hayotiy siklining barcha bosqichlarida ta’minlanishi kerak. Ma’lumotlarni yig‘ish bosqichida maxfiylik va

ma’lumot manbasining ishonchliligi, o‘qitish jarayonida ma’lumotlar yaxlitligi, modelni ishlab chiqishda kod va konfiguratsiya xavfsizligi, joriy etishda esa autentifikatsiya, avtorizatsiya, monitoring va jurnal yuritish muhim ahamiyat kasb etadi. Model yangilanganda yoki yangi ma’lumotlar bilan qayta o‘qitilganda ham xavfsizlik tekshiruvlari takrorlanishi lozim.

SI tizimlarining o‘ziga xos xususiyati shundaki, ularning chiqish natijasi faqat dastur kodi bilan emas, balki o‘qitish ma’lumotlari va model parametrlarining o‘zaro ta’siri bilan belgilanadi. Shu sababli hujumchi to‘g‘ridan-to‘g‘ri dastur kodini buzmasdan ham tizimga ta’sir ko‘rsatishi mumkin. Katta til modellari asosidagi chat-botlarda bunday xavflar ayniqsa dolzarbdir.

Xavfsizlik masalasini faqat model darajasida ko‘rish ham yetarli emas. Zamonaviy SI tizimlari ko‘pincha ma’lumotlar bazasi, bulutli servislar, API, hujjat omborlari va boshqa korporativ axborot tizimlari bilan integratsiya qilinadi. Natijada modelga berilgan ruxsatlar noto‘g‘ri sozlangan bo‘lsa, bitta zaif nuqta butun axborot tizimiga xavf tug‘dirishi mumkin. Demak, SI xavfsizligi korxonaning umumiy kiberxavfsizlik arxitekturasi bilan birgalikda boshqarilishi lozim.

1-rasm. Sun’iy intellekt tizimining hayotiy sikli va xavfsizlik nazorati.



2. Sun’iy intellekt tizimlariga xos asosiy kiberxavflar

Ma’lumotlar maxfiyligining buzilishi eng muhim xavflardan biridir. Foydalanuvchilar SI xizmatlariga ish hujjatlari, shaxsiy ma’lumotlar, tijorat sirlarini yoki texnik ma’lumotlarni yuborishi mumkin. Agar bunday ma’lumotlar qanday saqlanishi, qayta ishlanishi va uchinchi tomon xizmatlariga uzatilishi aniq belgilanmagan bo‘lsa, ma’lumotlarning nazoratsiz tarqalishi yuzaga keladi. Ayniqsa, korxona ichki hujjatlarini ommaviy AI xizmatlariga yuborishdan oldin ma’lumotlarni tasniflash va ruxsat siyosatini belgilash zarur.

Prompt injection hujumi katta til modellari uchun alohida xavf hisoblanadi. Bunda hujumchi modelga maxsus shakllantirilgan matn yuborib, uning dastlabki vazifasi yoki cheklovlarini chetlab o‘tishga harakat qiladi. Agar model tashqi vositalardan foydalanish, fayllarni o‘qish yoki API orqali amallarni bajarish imkoniyatiga ega bo‘lsa, bunday hujumning oqibati oddiy noto‘g‘ri javobdan ancha jiddiy bo‘lishi mumkin. Shu sababli modelga beriladigan huquqlar minimal darajada bo‘lishi, har bir tashqi amal alohida nazorat qilinishi va xavfli operatsiyalar uchun inson tasdig‘i talab etilishi kerak.

Ma’lumotlarni zaharlash hujumi ham SI xavfsizligining muhim muammolaridan biridir. Hujumchi o‘qitish yoki qayta o‘qitish ma’lumotlariga ataylab noto‘g‘ri namunalar kiritib, modelning ayrim holatlarda noto‘g‘ri qaror qabul qilishiga sabab bo‘lishi mumkin. Bunday xavfni kamaytirish uchun ma’lumot manbalarini tekshirish, ma’lumotlar to‘plamining versiyalarini nazorat qilish, o‘zgarishlar jurnalini yuritish va o‘qitishdan oldin sifat nazoratini o‘tkazish kerak.

Adversarial hujumlar, ya’ni modelga maxsus o‘zgartirilgan kirish ma’lumotlari orqali noto‘g‘ri natija chiqarishga undash ham ayrim amaliy tizimlar uchun xavf tug‘diradi. Masalan, tasvirni tanib olish tizimida inson ko‘ziga deyarli sezilmaydigan o‘zgarish model tasnifini o‘zgartirishi mumkin. Sanoat, transport yoki xavfsizlikka oid avtomatlashtirilgan qarorlarda bunday xatolar katta oqibatlarga olib kelishi ehtimoli mavjud. Shu bois muhim SI tizimlari muntazam ravishda stress-test, red-team sinovlari va mustaqil xavfsizlik baholashidan o‘tkazilishi maqsadga muvofiq.

Yana bir muhim xavf — noto‘g‘ri yoki uydirma axborot ishlab chiqarishdir. Katta til modellari ishonchli ko‘rinadigan, biroq faktlarga mos kelmaydigan javoblar berishi mumkin. Shuning uchun muhim qarorlar uchun AI natijasi inson tomonidan tekshirilishi va ishonchli manbalar bilan tasdiqlanishi kerak.

Izoh: jadval maqolaning 2-bo‘limida bayon qilingan xavf va tavsiyalar asosida tuzilgan; miqdoriy risk ballari berilmagan.

Xavf turi	**Maqolada tavsiflangan asosiy muammo**	**Tavsiya etilgan himoya chorasi**
Ma’lumotlar maxfiyligi	Maxfiy yoki tijorat ma’lumotlarining nazoratsiz tarqalishi	Ma’lumotlarni tasniflash, minimallashtirish va ruxsat siyosati
Prompt injection	Model ko‘rsatmalarini chetlab o‘tishga urinish	Minimal huquqlar, tashqi amallarni nazorat qilish, inson tasdig‘i
Ma’lumotlarni zaharlash	O‘qitish ma’lumotlariga noto‘g‘ri namunalar kiritish	Manbani tekshirish, versiyalar nazorati, sifat nazorati

1-jadval. Maqolada ko‘rsatilgan asosiy AI kiberxavflari va himoya choralarining umumlashtirilishi

3. Xavfsiz sun’iy intellekt tizimini yaratish tamoyillari

Birinchi tamoyil — xavfsizlikni tizimning boshidanoq loyihalashdir. “Security by design” yondashuvi bo‘yicha xavfsizlik funksiyalari tizim tayyor bo‘lgandan keyin qo‘shiladigan qo‘shimcha element emas, balki talablarni shakllantirish bosqichidan boshlab hisobga olinadigan omil sifatida qaraladi. Bunda aktivlar, tahdidlar, hujum ssenariylari va ehtimoliy zararlar aniqlanadi. Har bir SI loyihasi uchun xavf reyestrini shakllantirish va uni muntazam yangilab borish amaliy jihatdan foydalidir.

ikkinchi tamoyil — ma’lumotlarni minimallashtirish va tasniflash. Tizimga kerak bo‘lmagan ma’lumotni yig‘maslik, maxfiy ma’lumotni alohida belgilash va uni qayta ishlash qoidalarini ishlab chiqish xavfsizlikni sezilarli oshiradi. Korxonalarda “ochiq”, “ichki foydalanish uchun”, “maxfiy” va “juda maxfiy” kabi kategoriyalar asosida siyosat ishlab chiqish mumkin. AI xizmatlaridan foydalanish uchun

xodimlarga qaysi turdagi ma’lumotlarni yuborish mumkin yoki mumkin emasligi aniq ko‘rsatilishi kerak.

.*Uchinchi tamoyil* — doimiy monitoring va audit. SI tizimlarida foydalanuvchi so‘rovlari, model chaqiruvlari, API amallari, ruxsat o‘zgarishlari va muhim xatolar qayd etilishi lozim. Jurnallar markazlashtirilgan holda saqlansa, noodatiy faollikni aniqlash va hodisani tekshirish osonlashadi. Monitoring faqat hujum sodir bo‘lgandan keyin emas, balki normal foydalanish profilini aniqlash va undan og‘ishlarni vaqtida topish uchun ham xizmat qiladi.

4. Tashkiliy choralar va inson omilining roli

Texnik himoya vositalari qanchalik rivojlangan bo‘lmasin, xodimlarning xavfsizlik bo‘yicha bilimlari yetarli bo‘lmasa, tizimda zaiflik saqlanib qoladi. So‘nggi yillarda xodimlar AI vositalaridan matn tayyorlash, tarjima qilish, kod yozish, hujjatlarni tahlil qilish kabi vazifalarda faol foydalanmoqda. Bunday foydalanish tartibga solinmasa, maxfiy ma’lumotni tasodifan tashqi servisga yuborish ehtimoli ortadi. Shu sababli korxona AI foydalanish siyosatini ishlab chiqishi kerak.

Mazkur siyosatda ruxsat etilgan AI xizmatlari, taqiqlangan ma’lumotlar, ma’lumotlarni anonimlashtirish talablari, parollar va API kalitlarini himoyalash, hosil qilingan kontentni tekshirish, mualliflik huquqi masalalari va xavfsizlik hodisasi yuz berganda xabar berish tartibi belgilanishi mumkin. Xodimlarga faqat nazariy ma’ruza emas, balki real vaziyatlarga asoslangan qisqa amaliy mashg‘ulotlar o‘tkazish samaraliroq natija beradi. Masalan, xodimga soxta maxfiy hujjat berilib, undan AI xizmatidan foydalanish xavfsiz yoki xavfsiz emasligini aniqlash so‘ralishi mumkin.

Rahbariyat darajasida esa AI bilan bog‘liq xavflar umumiy axborot xavfsizligi risklari bilan birlashtirilishi kerak. Yangi AI tizimini sotib olish yoki ishlab chiqishdan oldin uning ma’lumot qayerda saqlanishi, provayderning xavfsizlik talablari, ma’lumotlardan ikkilamchi foydalanish shartlari, hodisalar haqida xabar berish tartibi va xizmat to‘xtagan taqdirda muqobil reja mavjudligi o‘rganilishi zarur. Shu tarzda texnologik qulaylik va xavfsizlik talablari o‘rtasida muvozanat yaratiladi.

5. O‘zbekiston sharoitida sun’iy intellekt xavfsizligi

O‘zbekistonda raqamli xizmatlar va sun’iy intellektdan foydalanish kengayib borayotgan sharoitda axborot xavfsizligi masalasiga tizimli yondashish muhim. Davlat tashkilotlari, banklar, ta’lim muassasalari va xususiy kompaniyalarda AI vositalari turli maqsadlarda joriy etilishi mumkin. Bunday jarayonda texnologiyani tez joriy qilish bilan bir qatorda, ma’lumotlarni himoyalash, foydalanuvchilar huquqlarini chegaralash va xavfsizlik hodisalariga javob berish mexanizmlari ham parallel ravishda shakllantirilishi kerak.

Ta’lim tizimida esa AI va axborot xavfsizligini birgalikda o‘rgatish kelajak mutaxassislarining raqamli kompetensiyasini oshiradi. Talabalar nafaqat AI vositalaridan foydalanishni, balki ularning xatolari, cheklovlari va xavfsizlik risklarini ham tushunishi kerak. Amaliy laboratoriya mashg‘ulotlarida phishing, prompt injection, parol xavfsizligi, ma’lumotlarni anonimlashtirish va xavfsiz API ishlatish kabi mavzularni simulyatsiya qilish mumkin. Bu yondashuv nazariy bilimni real vaziyatlarga tatbiq etishga yordam beradi.

6. Taklif va tavsiyalar

Birinchidan, tashkilotlarda AI tizimlarining yagona inventarini shakllantirish va har bir tizim uchun mas’ul shaxsni belgilash maqsadga muvofiq. Ikkinchidan, AI xizmatlaridan foydalanish bo‘yicha ichki siyosat ishlab chiqilib, maxfiy ma’lumotlar bilan ishlash talablari aniq belgilanishi kerak. Uchinchidan, AI tizimlariga kirishda ko‘p omilli autentifikatsiya, rollarga asoslangan ruxsat nazorati va eng kam imtiyoz tamoyili qo‘llanilishi lozim. To‘rtinchidan, model va ma’lumotlar o‘zgarishlarini nazorat qilish, versiyalarni saqlash hamda muntazam xavfsizlik testlarini tashkil etish zarur.

Beshinchidan, AI tizimlarida hodisalarni aniqlash va javob qaytarish rejasi ishlab chiqilishi kerak. Masalan, maxfiy ma’lumot tashqi servisga yuborilganligi aniqlansa, tegishli akkaunt yoki API kaliti darhol bloklanishi, hodisa qayd etilishi, ta’sir doirasi aniqlanishi va keyingi choralar belgilanadi. Oltinchidan, xodimlar uchun muntazam axborot xavfsizligi va AI savodxonligi treninglari tashkil etilishi lozim. Yettinchidan, muhim AI tizimlarida mustaqil audit va penetratsion sinovlardan foydalanish tavsiya etiladi.

Umuman olganda, xavfsiz AI uchun bitta universal texnik vosita mavjud emas. Samarali himoya qatlamli bo‘lishi kerak: ma’lumotlarni himoyalash, identifikatsiya va kirishni boshqarish, tarmoq himoyasi, model xavfsizligi, monitoring, audit, xodimlar tayyorgarligi va boshqaruv siyosati birgalikda ishlashi zarur. Risklar texnologiya rivojlanishi bilan o‘zgarib boradi, shuning uchun xavfsizlik nazoratlari ham muntazam ravishda qayta ko‘rib chiqilishi kerak.

Bosqich	**Asosiy faoliyat**	**Kutiladigan xavfsizlik nazorati**
1. Inventarizatsiya	AI tizimlari va ma’lumot manbalarini aniqlash	Tizimlar va ularga ulangan resurslar ro‘yxati
2. Risklarni aniqlash	Aktivlar, foydalanuvchilar, ruxsatlar va tahdidlarni belgilash	Risk reyestri
3. Nazoratlarni joriy etish	Texnik va tashkiliy himoya choralarini qo‘llash	MFA, RBAC, least privilege, API limitlari
4. Monitoring va audit	Jurnallar, noodatiy faollik va muhim amallarni kuzatish	Hodisalarga javob berish va doimiy nazorat
5. Trening va takomillashtirish	Xodimlar savodxonligi, test va mustaqil audit	Xavfsizlik madaniyati va muntazam yangilash

2-jadval. Korxonada AI xavfsizligini joriy etish bosqichlari

Xulosa

Sun’iy intellekt texnologiyalari axborot bilan ishlash samaradorligini sezilarli oshirish imkonini bermoqda, biroq ularning keng joriy etilishi yangi xavfsizlik muammolarini ham yuzaga keltirmoqda. Maxfiy ma’lumotlarning oshkor bo‘lishi, prompt injection, ma’lumotlarni zaharlash, modelni o‘g‘irlash, adversarial hujumlar va noto‘g‘ri natijalar AI tizimlarini loyihalash va ekspluatatsiya qilishda alohida e’tibor talab etadi. Ushbu xavflarni faqat dasturiy himoya bilan bartaraf etib bo‘lmaydi.

Kelajakda sun’iy intellekt va kiberxavfsizlikning o‘zaro bog‘liqligi yanada kuchayishi kutiladi. AI hujumlarni aniqlash va tahlil qilishda himoya vositasi sifatida ham ishlatilishi mumkin, biroq uning o‘zi hujumchilar tomonidan ham qo‘llanilishi ehtimoli mavjud. Shuning uchun texnologik rivojlanish bilan bir qatorda xavfsizlik madaniyatini rivojlantirish, mas’uliyatli foydalanish tamoyillarini joriy etish va inson nazoratini saqlab qolish muhim ahamiyatga ega.

Foydalanilgan adabiyotlar ro‘yxati

[1] National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST, 2023.

[2] National Institute of Standards and Technology. Cybersecurity Framework (CSF) 2.0. NIST, 2024.

[3] OWASP Foundation. OWASP Top 10 for Large Language Model Applications. OWASP, 2025.

[4] ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

[5] ISO/IEC 23894:2023. Information technology — Artificial intelligence — Guidance on risk management.

[6] Russell S., Norvig P. Artificial Intelligence: A Modern Approach. 4th ed. Pearson, 2021.

[7] Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016.

[8] European Union Agency for Cybersecurity (ENISA). Cybersecurity Challenges in the Era of Artificial Intelligence. ENISA analytical materials.

[9] Bishop C. M. Pattern Recognition and Machine Learning. Springer, 2006.

[10] Stallings W., Brown L. Computer Security: Principles and Practice. Pearson.

SUN’IY INTELLEKT TEXNOLOGIYALARINING TA’LIM TIZIMIDAGI O’RNI VA ISTIQBOLLARI. SUN’IY INTELLEKT VA AXBOROT XAVFSIZLIGI SOHASIDAGI ZAMONAVIY TAHDIDLAR VA ULARNING OLDINI OLISH CHORALARI

Aliboyeva Nilufar Iskandar qizi
Mirzo Ulug’bek nomidagi O’zbekiston Milliy universitetining
Jizzax filiali Amaliy matematika fakultetining
Amaliy matematika kafedrasi assistenti
gmail: nilufar.aliboyeva92@gmail.com

Annotatsiya. Bugungi kunda global raqamlashtirish davrida sun’iy intellekt (SI) texnologiyalari hayotimizning barcha jabhalariga, xususan, ta’lim tizimiga ham jadal kirib bormoqda. Zamonaviy ta’limda raqamli texnologiyalardan foydalanish nafaqat dars o’tish sifatini oshiradi, balki talabalarning mustaqil bilim olish imkoniyatlarini ham kengaytiradi. Mazkur tezisda sun’iy intellektning ta’lim jarayonidagi o’rni, uning afzalliklari va kelajakdagi istiqbollari tahlil qilinadi.